Le développement des TIC à l'épreuve de la sécurité

Pour le développement des technologies de l'information et de la communication, la sécurité de l'information et des réseaux s'est progressivement imposée comme un passage obligé. Partant de positions très différentes, les Etats membres et l'Europe évoluent vers des politiques de plus en plus cohérentes et complémentaires en matière de sécurité des systèmes d'information. L'établissement d'une base technologique, industrielle et opérationnelle compétitive et indépendante à l'échelle nationale et européenne est le nouvel objectif à viser.

par Alain Esterle (1)

Les fondements des politiques de sécurité des systèmes d'information

Le développement des technologies de l'information et de la communication s'accompagne d'un besoin croissant en politiques de sécurité destinées à préserver l'information (intégrité), à garantir ses conditions d'accès (disponibilité, confidentialité, identification des interlocuteurs) et sa valeur probante (authentification, imputabilité). Ces propriétés, regroupées sous le terme SSI (sécurité des systèmes d'information) ou *Infosec* en anglais (*information security*), sont essentielles pour garantir l'exercice autonome de la politique de l'Etat, ainsi que pour fonder la confiance des différents acteurs dans les grandes applications socio-économiques des technologies de l'information (échanges en ligne pour l'administration, le commerce, l'enseignement, la santé…).

Trois types d'acteurs sont concernés-:

--le citoyen, en tant qu'individu intéressé à la protection des données à caractère personnel, condition première des libertés individuelles dans les Etats démocratiques, et en tant que consommateur soucieux de la qualité des produits et services qu'il achète-;

--Les entreprises, dont le fonctionnement et la réussite – voire la survie – sont étroitement liés à la protection de leur savoir-faire, au respect des règles de propriété intellectuelle et de concurrence loyale, au bon déroulement des processus de production et de distribution-;

--L'appareil d'Etat en charge de la protection des informations sensibles, *a fortiori* des informations classifiées, ainsi que de la sécurité et de la continuité de fonctionnement des institutions et des infrastructures vitales pour les activités socio-économiques du pays-: la maîtrise des moyens de communications est plus que jamais un élément essentiel de la souveraineté.

Face à cette diversité d'acteurs et d'intérêts, les politiques de sécurité des systèmes d'information sont toujours des compromis (traduits en règles techniques, opérationnelles et juridiques) entre la préservation des libertés individuelles, des procédures de sécurité contraignantes et des allocations de ressources matérielles et humaines. Trois phases peuvent être distinguées-:

--la protection des systèmes d'informations qui porte sur le choix de produits de sécurité, les actions de contrôle et d'audit, les fonctions de veille et d'alerte ;

--la prévention-des incidents, notamment grâce à des actions de sensibilisation, de formation, de qualification de prestataires et à des exercices-;

--la capacité de réaction et de sanction, grâce à des équipes opérationnelles (CERT (2) ou CSIRT (3)), un appareil juridique spécifiant le caractère délictueux de certains actes et les services capables d'engager d'éventuelles poursuites.

Au cours des cinq ou six dernières années, des mutations profondes sont intervenues dans le paysage de la SSI tant au plan national qu'européen (1). Elles pourraient infléchir notablement le développement des TIC.

Les politiques nationales en matière de sécurité des systèmes d'information-: de fortes disparités institutionnelles sur fond d'un héritage commun

(1)-Alain Esterle a été Directeur adjoint à la Direction Centrale de la Sécurité des Systèmes d'Information du SGDN de décembre 1999 à août 2005. Le 1er septembre 2005, il a rejoint l'Agence européenne pour la sécurité des systèmes d'information (ENISA) comme Chef du Département Technique.

(2)-Computer Emergency Response Team (terminologie déposée par l'Institut Carnegie-Melon).

(3)-Computer Security Incident Response Team (sigle européen).

Au plan national, la sécurité des systèmes d'information apparaît comme un héritage de l'époque pas si lointaine où la cryptographie était considérée comme une arme que les Etats devaient maîtriser afin de protéger leurs informations militaires et diplomatiques les plus secrètes, et d'accéder à celles des Etats et groupes hostiles.

Depuis la fin des années 90, l'emploi généralisé des technologies de l'information et de la communication exige une pleine confiance de tous les acteurs dans la sécurité des systèmes. Il n'était plus possible de réserver les outils, méthodes et pratiques de sécurité aux seules fonctions régaliennes, ce qui a conduit à faciliter la fourniture et l'utilisation des moyens de cryptographie et le développement d'un marché ouvert en produits de sécurité.

Au plan institutionnel, le schéma général est le suivant-:

--une agence gouvernementale dispose de certaines prérogatives nationales (évaluation de la cryptographie, fabrication des clés…) et met des prestations de sécurité à disposition de l'ensemble des ministères, qui restent responsables de la SSI de leurs réseaux,

--une autre instance (autorité de régulation des télécommunications, par exemple) est en charge de la SSI pour les applications «-civiles-» de la société de l'information.

Il peut se faire que l'agence gouvernementale englobe l'ensemble des responsabilités de la politique de SSI (cas de la DCSSI en France, l'ART n'ayant pas de responsabilité en SSI). Mais il arrive aussi, souvent, que cette agence reste, comme aux Etats-Unis, intégrée dans les services de renseignement sur les communications ou SIGINT (4) (Espagne, Royaume-Uni, Pays-Bas). Par ailleurs, cette agence peut être rattachée directement au chef du gouvernement (France, Espagne) ou faire partie d'un ministère particulier (Intérieur en Allemagne, Affaires étrangères au Royaume-Uni). Elle entretient le plus souvent des relations étroites avec l'instance gouvernementale en charge du développement de l'administration électronique (eEnvoy au Royaume-Uni, ADAE en France).

Malgré quelques différences de périmètres, les ressources humaines de ces agences peuvent être considérées comme un bon révélateur de la priorité politique accordée à ces questions-: environ 3-000 personnes travaillant à la Division Information Assurance de la NSA, aux Etats-Unis, 400 au Bundesamt für Sicherheit in der Infromationstechnik (BSI) en Allemagne et au Commununications Electronics Security Group (CESG) au Royaume-Uni, et 100 personnes à la DCSSI, en France.

Les capacités de développement et d'évaluation des produits de sécurité-: un besoin partagé au niveau national

Le marché des produits commerciaux assurant des fonctions de sécurité des communications électroniques est aujourd'hui largement dominé par un nombre limité de fournisseurs non européens. Cette situation de quasi-monopole peut avoir des répercutions très négatives en termes tant de concurrence que de sécurité.

Des procédures d'évaluation ont été mises en place pour garantir au consommateur que le produit qu'il achète fait bien ce qu'il est censé faire (mais sans garantir qu'il ne puisse aussi faire autre chose…), notamment résister à certaines attaques. Les agences gouvernementales sont largement impliquées dans ces procédures-:

--elles réalisent pratiquement toutes les évaluations des produits cryptographiques en interne-;

--dans le domaine du contrôle des signaux compromettants (TEMPEST), la tendance actuelle est à l'externalisation des évaluations,-celles-ci étant alors simplement sous-traitées ou réalisées chez les industriels, sous contrôle étatique-;

--l'évaluation des produits de sécurité des technologies de l'information, plus récente, a dès le début été réalisée par des laboratoires privés agréés par les agences nationales en SSI, sur la base de standards publics tels que les Critères communs (norme ISO 15408) et plus récemment le FIPS140-2 proposé par le NIST (5) américain-;

--ce travail d'évaluation est validé par un centre de certification qui délivre *in fine* un certificat (schéma d'évaluation/certification). Cette fonction est assurée par l'agence gouvernementale, même si peuvent exister simultanément des organismes privés de certification (TUV-IT et T-System en Allemagne, par exemple)-;

--un accord de reconnaissance mutuelle, signé en 1999 entre les Etats membres, valide pour tous les évaluations/certifications faites chez l'un d'eux, quel qu'en soit le niveau, excepté les équipements traitant d'informations classifiées. Sur le plan international, le «-Common Criteria Mutual Recognition Agreement-» adopté en mai 2000 permet de reconnaître les certificats selon les critères communs délivrés par n'importe quel pays signataire, jusqu'au niveau EAL 4.

Compte tenu des garanties limitées qu'offrent ces procédures d'évaluation, la plupart des Etats membres essaient de préserver une certaine diversité d'approvisionnement, par exemple en favorisant le développement de filières fondées sur des sources ouvertes (logiciels libres) et/ou en assurant un contrôle direct sur le développement de certains produits, notamment les équipements cryptographiques de haut niveau de sécurité. Comme aux Etats-Unis, c'est généralement l'agence nationale en SSI qui est chargée du développement de ces produits (Allemagne, Pays-Bas, Royaume-Uni, Espagne). En France, cette activité est actuellement assurée par la Délégation générale pour l'Armement (DGA) du ministère de la Défense.

Les services en sécurité des systèmes d'information-: un marché qui tend à se réguler

Les services traitant de la SSI se sont largement développés ces dernières années. A la traditionnelle gestion des

(4)-Signal Intelligence.
(5)-National Institute for standards and Technology.

clés cryptographiques se sont ajoutés le conseil (assistance à maîtrise d'ouvrage), la réalisation d'audits techniques de sécurité, l'exploitation de la sécurité des réseaux, la certification des clés racines des IGC, avec, dans chaque cas, la nécessité d'une grande confiance entre le commanditaire et le prestataire.

La gestion des clés cryptographiques reste traditionnellement une des activités les plus contrôlées. Ainsi le CESG (pour le Royaume-Uni), la NSA (pour le DoD américain), DACAN (pour l'OTAN), le NLNCSA (pour les Pays-Bas) ont encore le monopole de la fabrication des clés de confidentialité pour l'administration, avec toutefois une certaine tendance à la décentralisation compte tenu de la lourdeur de cette fonction.

Pour les-services plus récents, les besoins croissants des secteurs tant public que privé ont fait émerger un grand nombre de prestataires privés et le besoin d'un label de qualité pour leurs prestations. Le CESG britannique a été le premier à s'engager dans cette voie, avec notamment les programmes de qualification des consultants CLASS et le programme IT-Health Check pour la réalisation d'audits techniques des systèmes d'information. De même, le BSI a mis récemment en place un programme d'accréditation des auditeurs selon son standard d'audit des systèmes d'information (I). En France, le Plan de renforcement de la sécurité des systèmes d'information de l'Etat (II) prévoit des mécanismes de qualification de prestataires privés, notamment en audit et conseil. Cette régulation progressive du marché des services en SSI s'appuie sur des standards, dont le plus connu est l'ISO 17799.

Les capacités de réaction aux attaques et de protection des infrastructures critiques-: des approches nationales publiques et privées qui gagneront à être mieux coordonnées

Depuis la fin des années 90 se sont progressivement développées au sein des Etats membres des structures opérationnelles et juridiques destinées à réagir plus efficacement aux attaques sur les réseaux et à mieux protéger les infrastructures critiques nationales. Ces structures sont principalement de trois catégories-:

--des équipes techniques de statut public ou privé, de type CERT (6) ou CSIRT (7) pour la veille, l'alerte et la réaction aux attaques-;

--des services de type CCU (8) en charge des poursuites des délits liés à l'emploi des technologies de l'information et de la communication-;

--des structures dédiées à la protection des infrastructures critiques et des plans de vigilance et d'intervention adaptés aux attaques contre les réseaux, jusqu'au plus haut niveau d'intensité.

Après l'abandon du projet d'EuroCERT (1999-2000), des structures autonomes à statut universitaire, gouvernemental ou commercial se sont progressivement mises en place au sein des Etats membres, pour assurer les fonctions de veille, alerte et réaction aux attaques. On compte actuellement quelques 80 CSIRTs en Europe, regroupés au sein de la structure de coordination TF-CSIRT qui a notamment des activités de formation (création de nouveaux CSIRTs), de normalisation (catégorisation des incidents) et de mise au point de liaisons sécurisées en toutes circonstances. Un accent particulier est mis sur la disponibilité de moyens de veille et d'alerte au service des PME. D'autres structures de coordination existent à l'échelle mondiale (FIRST) et entre les CSIRTs gouvernementaux de certains Etats membres de l'Union européenne (European governmental CSIRTs).

Le besoin de lutter contre la cyber-criminalité a conduit la plupart des Etats membres à instaurer des unités spécialisées, couramment appelées CCU (Computer Crime Units), pour mener en tant que de besoin, et en s'appuyant sur l'expertise technique des CSIRTs, des poursuites judiciaires relatives aux attaques contre les réseaux ou à des délits plus traditionnels ayant impliqué les communications électroniques.

La plupart de ces équipes restent de petites dimensions, au regard de l'ampleur de la tâche et une bonne partie de leur activité consiste à coordonner les actions d'autres équipes d'investigation (BundesKriminalamt ou BKA en Allemagne). Au Royaume-Uni, la structure nationale NHTCU (9) assure la coordination avec des correspondants locaux à l'échelle du pays, la coopération entre agences et des liaisons avec les industries. En France, ce rôle est assuré depuis mai 2000 par l'OCLCTIC (10) créé au sein de la Direction générale de la Police nationale du ministère de l'Intérieur.

D'une manière générale, ces CCUs sont confrontées à des besoins de croissance interne, de coordination entre elles et de coopération opérationnelle avec leurs homologues étrangères (investigations au-delà des frontières). Des réseaux de points de contact nationaux avec certaines instances internationales (Europol, Interpol, G8) ont été mis en place pour améliorer la coordination de leurs actions.

Les Etats membres sont aussi confrontés au risque d'attaques majeures contre les réseaux, susceptibles de paralyser ou d'endommager durablement certaines infrastructures essentielles à la continuité des activités socio-économiques du pays-: télécommunications, transports, énergie, santé, système bancaire, etc. La protection de ces infrastructures « critiques-» s'appuie aussi largement sur les compétences et les structures de coordination dont disposent les CSIRTs.

Ainsi au Royaume-Uni, le NISCC (11), rattaché au Home Office, s'appuie sur l'UNIRAS (CSIRT gouvernemental) pour fournir aux opérateurs des infrastructures critiques des avis techniques et des informations sur les menaces, les vulnérabilités et les niveaux d'alerte. Il s'appuie aussi sur des WARPs (12), chargés de recueillir des alertes et de signaler des incidents (mais sans capacité d'intervention) et des ISAC (13), qui

(6)-Computer Emergency Response Team (terminologie déposée par l'Institut Carnegie-Mellon).
(7)-Computer Security Incident Response Team (sigle européen).
(8)-Computer Crime Unit.
(9)-National High Technology Crime Unit.
(10)-Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.
(11)-National Infrastructure Security Co-ordination Centre.
(12)-Warning, Advice and Reporting Point.
(13)-Information Sharing and Analysis Center.

diffusent des informations d'alerte et d'incidents au sein d'une communauté donnée d'utilisateurs, généralement sur une base commerciale.
En Allemagne, la protection des infrastructures critiques est confiée au BSI qui a entrepris un travail d'identification de ces infrastructures, grâce à des exercices impliquant l'administration (ministères de l'intérieur, de la défense, des transports, des télécommunications) et des industriels (EADS).
En France, le pilotage général de la protection des infrastructures vitales est confié au Secrétariat général de la Défense nationale, avec un rôle particulier pour le COSSI (centre opérationnel en SSI qui englobe le CERTA, le CSIRT gouvernemental français). La politique de protection comprend des inspections pratiquées régulièrement sur un ensemble de points et réseaux sensibles répartis sur le territoire, des plans de vigilance et d'intervention qui sont déclenchés lorsque les menaces augmentent significativement et des exercices impliquant tout ou partie de l'appareil d'Etat et des infrastructures critiques.
De plus en plus, ces activités nationales s'élargissent à des actions coordonnées au plan international (*Table top exercice* impliquant les pays du G8 en mai 2005) et européen, avec notamment la préparation d'un Programme européen de protection des infrastructures critiques (EPCIP) s'appuyant sur le réseau d'alerte CIWIN (III).

L'Union européenne et la sécurité des systèmes d'information-(SSI) : une politique en devenir

Contrairement aux Etats membres, les institutions européennes n'ont pas d'héritage historique en matière de protection d'information classifiée ni d'activité de renseignement (IV)-: la politique actuelle de l'Union en matière de SSI s'inscrit d'abord dans le sillage de la politique économique et monétaire développée depuis 50 ans, au regard de la politique européenne de sécurité et de défense (PESD), beaucoup plus récente.
On peut considérer comme élément fondateur de l'engagement européen en matière de SSI la «-stratégie de Lisbonne-», adoptée par le Conseil en mars 2000 (14) afin que l'Union puisse-«-*devenir l'économie de la connaissance la plus compétitive et la plus dynamique du monde, capable de croissance économique durable accompagnée d'une amélioration quantitative et qualitative de l'emploi et d'une plus grande cohésion sociale*-», sur la base d'un emploi généralisé et fiable des technologies de l'information et de la communication. Depuis lors, la pression du contexte géopolitique a conduit l'Union à aborder d'autres domaines de la SSI.

Le développement d'un cadre juridique européen à même de renforcer la confiance des acteurs

En préambule à un espace unique européen d'information (objectif du programme i2010 en gestation), les directives du «-paquet télécom-» ont renforcé le socle juridique de la sécurité des communications électroniques en Europe, notamment en matière-:
--d'intégrité et sécurité des réseaux, qui doivent être garanties par les autorités nationales de régulation (directive cadre 2002/21)-;
--d'accès au réseau pour tous et en particulier aux services d'urgence pour lesquels les Etats membres doivent prendre toutes les mesures nécessaires (directive «-service universel-» 2002/22), à charge pour les autorités de régulation de fixer les techniques et les méthodes opérationnelles auxquelles les fournisseurs devront se soumettre (directive «-accès-» 2002/19)-;
--d'interception légale et d'utilisation en cas de catastrophe majeure, qui font partie des obligations spécifiques conditionnant les autorisations de fourniture de réseaux et de services de communication électroniques (directive « autorisation-» 2002/20)-;
--de protection des données à caractère personnel, que les autorités nationales de régulation doivent contribuer à assurer à un niveau élevé (directive « cadre-» 2002/21).
L'édifice a été complété par la directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée, notamment la confidentialité des communications électroniques à caractère public, qui doit être garantie par les Etats membres, ainsi que les messages non sollicités ou *spam,* pour lesquels le principe de l'autorisation préalable (*opt-in*) est retenu. En matière d'imputabilité, la directive 1999/93 donnait déjà à la signature électronique la même valeur légale qu'à la signature manuscrite. Quant à la protection des personnes physiques, au regard du traitement des données personnelles et de leur libre circulation, elle est assurée par la directive 1995/46.
En ce qui concerne la conservation des données de connexion associées aux communications électroniques (mais qui ne concernent pas leur contenu), déjà abordée dans la directive 2002/58, l'adoption de la déclaration sur la lutte contre le terrorisme consécutive aux attentats du 11 mars 2004 à Madrid a conduit beaucoup d'Etats membres à légiférer et quatre d'entre eux (France, Irlande, Royaume-Uni et Suède) ont proposé une série de principes qui, repris pas la Commission sous forme de directive, devraient être adoptés d'ici la fin 2005.
Sur ces bases, le travail consiste surtout à suivre la mise en œuvre des textes (transposition dans les législations nationales) et à débattre des ajustements souhaitables (révision tous les trois ans environ).

Des programmes de R&D

(14)-Avant 2000, la Commission avait mis en place un Senior Officer Group sur la société de l'information (SOG-IS) dont les recommandations ont conduit à l'adoption en 1997 d'un Accord de Reconnaissance Mutuelle sur l'emploi des critères ITSEC pour l'évaluation des outils de sécurité, puis à son extension aux critères communs en 1999 (cf. supra). On peut aussi noter l'adoption de la directive sur le signature électronique, fin 1999.
(15)-Le budget total du 6e PCRD s'élève à 17,5 milliards d'euros (y compris Eurotam) sur la période de 2002-2006. Par comparaison, le 5e PCRD a représenté une enveloppe de 15 milliards d'euros de 1998 à 2002, dont 3,6 pour les technologies de la société de l'information. Le budget du 7e PCRD est en discussion (débat sur le budget de l'Union de 2007 à 2013, avec une proposition initiale de la Commission à 73 Mds€, dont 28 % sur les TIC, 10 % sur la sécurité).

élargis à certaines applications duales

Sur les 3,62 milliards d'euros du 6e programme cadre de R&D (PCRD) consacrés aux ICT (20 % du total) (15), 50 millions d'euros environ concernent le thème «-Vers un cadre global de confiance et de sécurité-». Dans la préparation du 7e PCRD, on notera un budget accru consacré aux ICT (28 % peut-être), la confiance et la sécurité restant un thème prioritaire ciblé (parallèlement au soutien au commerce et à l'industrie, aux contenus, techniques d'apprentissage et nouveaux media, aux grands enjeux sociaux).

A partir de 2004, et sur la base d'un rapport validé par 25 personnalités européennes, la Commission a engagé une Action préparatoire sur les recherches en sécurité (PASR) portant sur les moyens techniques de lutte anti-terroriste, la prévention et la réaction contre les armes de destruction massive (16) et la protection des réseaux d'information. Dotée d'un faible montant de crédits (12,5 millions d'euros en 2004, autant en 2005), elle vise surtout à préparer un programme européen de recherches en sécurité (EPSR), qui doit être intégré au 7e PCRD. Il s'agit d'un tournant majeur de par son volume (dotation attendue de l'ordre du milliard d'euros) mais surtout parce que les thèmes traités sortent du cadre traditionnel (soutien au marché intérieur, applications civiles) et concernent clairement les second et troisième piliers.

Les responsabilités croissantes de l'Union en matière opérationnelle

A la suite du programme IDA (Interchange of Data between Administrations), devenu IDABC (17), la Commission européenne a entrepris fin 2003 de développer TESTA (18), réseau européen reliant les réseaux nationaux des administrations des Etats membres. La Commission, maître d'ouvrage, est aujourd'hui amenée à définir une politique de sécurité propre à TESTA, à spécifier avec les Etats membres les conditions techniques et opérationnelles d'interconnexion entre TESTA et les réseaux nationaux et à mettre en place une procédure d'homologation de réseaux impliquant les partenaires nationaux.

D'abord simple coordinatrice des travaux préparatoires du programme Galileo (études de faisabilité financées sur le 5e PCRD), la Commission a progressivement réduit son rôle au profit de l'ESA (co-pilotage de l'étude de définition), puis de l'Entreprise commune (phase de développement) et enfin de l'Autorité de surveillance Galileo (phase de déploiement). En revanche, le rôle du Secrétariat général du Conseil s'est progressivement affirmé en tant qu'autorité politique européenne légitime pour la gestion opérationnelle des enjeux de sécurité liés à Galileo, en particulier pour les prises de décision nécessairement très rapides en période de crise telles que celle de dégrader certains signaux, de les rendre inaccessibles à certains utilisateurs, de les supprimer, de les rétablir, etc.

Enfin le Secrétariat général du Conseil a été confronté à la gestion du réseau ESDPnet (European security and Defence Policy), fusion des réseaux opérationnels WEUnet de l'UEO ainsi que de Cortesy reliant les ministères des Affaires étrangères des Etats membres, les représentations permanentes, la Commission et le Secrétariat du Conseil à Bruxelles. Les accords de reconnaissance mutuelle dans l'évaluation de produits de sécurité ne s'appliquant pas à la protection des données classifiées, le Secrétariat a fait adopter en décembre 2002 par les Etats membres le CISPS (Council Infosec Selection and Procurement Scheme) qui prévoit qu'un équipement développé par un Etat membre donné sera valablement évalué par une AQUA (Appropriately Qualified Authority) relevant d'un autre Etat. De plus, l'OTAN et l'Union européenne ont signé à Athènes le 14 mars 2003 un accord sur la sécurité de l'information, ouvrant la voie à l'échange d'informations classifiées, complété le 3 juin 2003 par la définition de standards communs pour la protection des informations classifiées, y compris pour les équipements utilisant des systèmes de cryptographie.

Le rôle attendu de l'agence européenne pour la sécurité de l'information et des réseaux

En matière de sécurité, le programme eEurope, en vigueur de 2000 à 2005 pour soutenir la stratégie de Lisbonne, aura eu au moins un résultat majeur-: la création de l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) (19).

Il est attendu d'ENISA qu'elle devienne un centre d'expertise capable *«-d'assister la Commission, les Etats membres et le secteur des entreprises en vue de les aider à satisfaire aux exigences de sécurité des réseaux et de l'information-»* et de *«-renforcer la coopération entre les différents acteurs dans le domaine de la sécurité des réseaux et de l'information-»*. Une des premières tâches d'ENISA consistera à dresser un catalogue des compétences réparties au sein de l'Union pour l'ensemble des métiers de la sécurité des systèmes d'information.

Elle devra aussi assurer la-«-*promotion des meilleures pratiques, y compris les méthodes d'alerte des utilisateurs… fournir à la Commission des conseils sur la recherche en matière de sécurité des réseaux et de l'information…* et *suivre l'élaboration* [des normes] *pour les produits et services*-» en SSI.

Il est bien sûr trop tôt pour apprécier la place qu'ENISA est appelée à prendre dans le développement des politiques de SSI au sein de l'Union et au-delà. L'année 2005 sera surtout consacrée à l'implantation de l'agence à Héraklion (Crète), à la démonstration de ses capacités à mener des actions de sensibilisation et de concertation entre les acteurs concernés et à la consolidation

(16)-Nucléaire, Radiologique, Bactériologique et Chimique (NRBC).

(17)-Fourniture interopérable de services paneuropéens de gouvernement électronique aux administrations publiques, aux entreprises et aux citoyens (IDABC).

(18)-Trans-European Services for Telematics between Administrations.

(19)-Règlement n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004, instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information – JO de l'UE, L77/1 à 11 du 13 mars 2004.

de ses compétences dans le domaine de la SSI.
Quoi qu'il en soit, ENISA peut devenir à terme un acteur précieux d'harmonisation des politiques et des pratiques de la SSI à l'échelle de l'Union, facteur de réduction des disparités de compétences techniques et opérationnelles entre les pays membres, voire entre les acteurs au sein d'un même pays. Dans ce sens, elle est appelée à jouer un rôle majeur dans l'élévation du niveau général de la sécurité de l'information et des réseaux dans l'ensemble de l'Union.

Les nouveaux enjeux de la SSI pour la société de l'information en France et en Europe

Avec la convergence informatique-télécommunications qui s'approche et le passage au «-tout IP-», les enjeux de sécurité des réseaux et de l'information doivent maintenant être réévalués à l'horizon des dix à quinze années à venir. Alors que la Commission européenne propose d'élaborer en 2006 une «-Stratégie pour une société de l'information sûre-» (voir COM(2005) 229 final), deux documents récents analysent les enjeux de SSI à moyen terme et proposent une dizaine d'actions prioritaires. On peut noter que le comité consultatif en technologies de l'information du président américain (V) et le séminaire européen sur la sécurité d'Internet (VII) identifient quelques objectifs similaires-:
--une meilleure coordination des politiques et plans d'action, entre les Etats membres et les agences fédérales respectivement-;
--un emploi plus systématique de méthodes rigoureuses pour inclure les exigences de sécurité dans la conception, le développement et la validation des logiciels de commerce-;
--des actions de sensibilisation pour améliorer la culture de sécurité et pour partager les expériences-;
--des méthodes et des moyens techniques nouveaux à la mesure de la complexité croissante des réseaux et des interconnexions.
Néanmoins, en vue des analyses stratégiques à venir aux niveaux national et européen, deux points méritent une attention particulière, en raison de leurs implications sociales et économiques.
La gestion des identités est un champ où s'entrecroisent la protection des données personnelles, la recherche de profits économiques et les actions de lutte contre la grande criminalité et les actions terroristes. Le terrorisme international et les gains de productivité associés aux technologies de l'information sont devenus deux tendances lourdes pour le moyen terme, alors que la vision européenne de la protection des données personnelles (directive 1995/46), bien que dominante à l'échelle mondiale, est toujours confrontée à une conception américaine beaucoup plus limitative en matière de protection. Une inflexion de cette position européenne, sous la pression des deux tendances lourdes évoquées plus haut, pourrait avoir des conséquences majeures en matière d'équilibre social et politique dans le contexte européen (VII).

L'enjeu de souveraineté que représente la maîtrise des moyens de communication doit être adapté au contexte qui se prépare, avec deux conséquences concrètes

D'une part la gouvernance d'Internet devient un enjeu politique majeur, comme le confirme la décision du département du commerce américain de maintenir ses relation privilégiées avec l'ICANN (VIII). La mise en place d'une capacité réellement autonome de gestion des adresses et noms de domaines doit être identifiée comme un enjeu majeur au niveau national et européen et se traduire dans les faits.
D'autre part, le caractère stratégique de la base technologique et industrielle en SSI doit être reconnu comme tel, ce qui demande des inflexions majeures en matière de soutien à l'innovation, de recherche de compétitivité, des actions publiques volontaristes en matière de développement de produits et services de haut niveau en SSI, des adaptations organisationnelles, voire institutionnelles. Au plan national français, cette problématique s'inscrit clairement dans le sillage du rapport du député Carayon (20), ainsi, plus récemment que de la mission confiée au député Lasborde (La Tribune, 8 juillet 2005). La préparation de la nouvelle tranche du Plan de renforcement de la sécurité des systèmes d'information devrait être l'occasion de sa traduction concrète. La préparation prochaine d'une «-stratégie pour une société de l'information sûre-» pourra également être l'occasion de sa prise en compte au niveau européen. ●

(20)-Htpp://w.ladocumentationfrancaise.fr.rapports-publics/034000484/index.shtml

BIBLIOGRAPHIE

(I)-IT Baseline Protection Manual, Federal Office for Information Security (BSI), http://www.bsi.de/english/gshb/manual/

(II)-Plan de renforcement de la sécurité des systèmes d'information, SGDN, 10201/SGDN/SG, 17 octobre 2003.

(III)-Séminaire sur la protection des infrastructures critiques, Union européenne, Bruxelles, 6-7 juin 2005.

(IV)-M.-Lemoine, recommendation 707 «-On the new challenges facing European Intelligence-», Western European Organization Assembly, 2002.

(V)-«-Cyber security-: a crisis of prioritization-», President's Information Technology Advisory Committee (PITAC), février 2005.

(VI)-Séminaire sur la Sécurité d'Internet, Commission européenne, DG INFSO-A3, mai 2005.

(VII)-Alain Esterle, «-ICT security stakes and identity management in the future Europe-», Conférence Fistera, Séville, 16-17 juin 2005.

(VIII)-US principles on the Internet's domain name and addressing system, National Telecommunication and Information Administration, 30 juin 2005.